N

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,540	10/07/2003	Chih-Pen Chang	ALIP0015USA	2539

27765 7590 11/21/2006

NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION
P.O. BOX 506
MERRIFIELD, VA 22116

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/605,540	**Applicant(s)** CHANG ET AL.	
	Examiner Paula W. Klimach	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/16/05*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claim Objections

Claim 8 is objected to because of the following informalities: "sequentiallygenerated" should be "sequentially generated". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 4, 7-8, 14, and 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Garcken et al (5,778,074).

In reference to claim 1 Garcken discloses a system for generating variable substitution boxes from arbitrary keys for use in a block cipher system utilizes an initial set of linearly independent numbers to generate substitution tables (abstract). The system includes a key-receiving module comprising an N-bit register which comprises m groups of registers for receiving an N-bit key which comprises m groups of keys, the m groups of keys stored in the m groups of registers respectively, both of N and larger than two (Fig. 2B parts 104 and column 11 lines 11-18); and an inverse key evaluation m being power-of-two integers module comprising m XOR logic gates and a digital data processing module for inversely evaluating to generate a plurality of pre-keys in sequence according to the keys received by the key receiving module (column 11 lines 39-43), wherein the XOR network is made of a variable number of XOR gates and therefore suggest m XOR gates; wherein the keys stored in the N-bit register are replaced in sequence by the pre-keys which are obtained by utilizing the inverse key evaluation module to process the keys once (part 111 Figure 2B), wherein evaluation only occurs once because the value that is RSLT will change for the next pass.

In reference to claim 4 Garcken discloses a system wherein the inverse key evaluation circuit of claim 1 wherein the inverse key evaluation circuit further comprises a register electrically connected to the inverse key evaluation module for storing a key obtained through one inverse key evaluation, wherein the key storing in the register is replaced by a prek-key generated from the key through one inverse key evaluation (part 138 Fig. 2C).

In reference to claim 7 Garcken discloses a system for generating variable substitution boxes from arbitrary keys for use in a block cipher system utilizes an initial set of linear ly independent numbers to generate substitution tables (Abstract). The system of Garcken includes providing a key and the enciphered text string (part 138 Fig. 2C); utilizing an inverse key evaluation module to sequentially generate a plurality of pre-keys of the key (column 10 line 63 to column 11 line 10); and using the key and the pre-keys generated from the key to perform a plurality of corresponding decryption operations for decrypting the enciphered text string to the plain text string (column 11 lines 28-33).

In reference to claim 8 Garcken discloses a system wherein the method further comprises using a register to store the key and the prekeys sequentially generated from the key, the key stored in the register is sequentially replaced by a next pre-key which is obtained by utilizing the inverse key evaluation module to process the key once (part 138 Figure 2C).

In reference to claim 14 Garcken discloses a system for generating variable substitution boxes from arbitrary keys for use in a block cipher system utilizes an initial set of linear ly independent numbers to generate substitution tables (Abstract). The system of Garcken discloses a system that includes a key-generating module for providing a plurality of keys, the key-generating module, comprising: a forward key evaluation circuit for generating a plurality of post-keys of a original key according to the original key until generating the last key (column 10 lines 4-14); an inverse key evaluation circuit for generating a plurality of pre-keys of the last post key according to the last post-key until generating the original key (column 6 lines 2-5); and at least one register for storing the original key and the last post-key (part 138 Fig. 2C); an encryption module electrically connected to the key-generating module for sequentially performing a plurality of corresponding encryption operations according to the original key and the post-keys sequentially generated, which are provided by the forward key evaluation circuit, to encrypt a plain text string to a corresponding enciphered text string (column 11 lines 28-33); and a decryption module electrically connected to the key-generating module for sequentially performing a plurality of corresponding decryption operations according to the last post-key and the prekeys sequentially generated, which are provided by the inverse key evaluation circuit, to decrypt an enciphered text string to a corresponding plain text string (column 11 lines 28-33).

In reference to claim 17 The system includes a key-receiving module for receiving the last key (part 138 Fig. 2C); an inverse key evaluation module comprising a plurality of XOR logic gates and a digital data processing module for generating a plurality of pre-keys according to the last key received by the key-receiving module until generating the original key (Fig. 2B); and a register electrically connected to the inverse key evaluation module for storing a key obtained through one inverse key evaluation, the key stored in the register replaced by a pre-key obtained from the key through one inverse key evaluation (part 138 Fig. 2C).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 5, 9-10, 12, 15-16, 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Garcken et al in view of the article by Nechvatal et al ("Report on the Development of the advanced encryption standard").

In reference to claim 2 wherein the value of N is 128 and the value of m is 4, the key received by the key-receiving module at first is inverse evaluated ten times to generate ten prekeys in order. Garcken discloses the key received by the key-receiving module at first is inverse evaluated ten times to generate ten prekeys in order (column 6 lines 19-34). Gracken teaches generating a set of linearly independent numbers (prekeys), and as a result the set may be a set of 10.

Although Garcken discloses a key stored in a key register and the formation of n-bit S Tables for use in encryption, thus leaving the number of values open to include ten prekeys, however Garcken does not disclose the value of N is 128 and the value of m is 4.

Nechvatal discloses the minimum requirement for AES is a N is a value of 128 so that the key has a length of 128 bits (1.1 Background) and the test for the AES were performed on a 32 bit processor (section 3.3.1 Machine Word Size) therefore the 4 group register (m is a value of 4) is convenient to work with the 32 bit processor.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a key with a bit size of 128 and a value of 4 for the groups. One of ordinary skill in the art would have been motivated to do this because the minimum requirements for AES are a key size of 128 and the processor used to test AES candidates is a 32 bit processor. AES is a system that will be used to secure sensitive government information (Nechvatal 1. Overview of the Development Process for the Advanced Encryption Standard and Summary of Round 2 Evaluations) and as a result will greatly influence other systems for securing information.

In reference to claims 5, 12, and 18 wherein the cryptosystem is qualified to an advanced encryption standard (AES).

Although Garcken discloses a block cipher, Garcken does not disclose system wherein the cryptosystem is qualified to an advanced encryption standard (AES).

Nechvatal discloses the minimal requirements to qualify for an advanced encryption standard (Section 1.1 Background).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to to qualify the cryptosystem for an advanced encryption standard as taught by Nechvatal in the system of Gracken. One of ordinary skill in the art would have been motivated to do this because AES is a system that will be used to secure sensitive government information (Nechvatal 1. Overview of the Development Process for the Advanced Encryption Standard and Summary of Round 2 Evaluations) and as a result will greatly influence other systems for securing information

In reference to claim 9 wherein the key is a N-bit key, in which N is equal to 128, and 10 pre-keys can be obtained in order from the key via the inverse key evaluation module. Garcken discloses the key received by the key-receiving module at first is inverse evaluated ten times to generate ten prekeys in order (column 6 lines 19-34). Garcken teaches generating a set of linearly independent numbers (prekeys), and as a result the set may be a set of 10.

Although Garcken discloses a key stored in a key register and the formation of n-bit S Tables for use in encryption, thus leaving the number of values open to include ten prekeys, however Garcken does not disclose the value of N is 128.

Nechvatal discloses the minimum requirement for AES is a N is a value of 128 so that the key has a length of 128 bits (1.1 Background).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a key with a bit size of 128 as in Nechvatal in the system of Garcken. One of ordinary skill in the art would have been motivated to do this because the minimum requirements for AES are a key size of 128 and the processor used to test AES candidates is a 32 bit processor. AES is a system that will be used to secure sensitive government information (Nechvatal 1. Overview of the Development Process for the Advanced Encryption Standard and Summary of Round 2 Evaluations) and as a result will greatly influence other systems for securing information.

In reference to claim 10 Garcken discloses a system wherein the inverse key evaluation module comprises m XOR logic gates (part 113 Fig. 2B) and a digital data processing module to perform a plurality of inverse key evaluations according to the key and sequentially generate a plurality of pre-keys corresponding to the key, m being a power-of-two integer larger than two (column 6 lines 2-5).

In reference to claim 16 wherein the plain text string, the enciphered text string, and the plurality of keys are all 128-bit digital data.

Although Garcken discloses a key stored in a key register and the formation of n-bit S Tables for use in encryption, thus leaving the number of values open to include ten prekeys, however Garcken does not disclose the value of N is 128.

Nechvatal discloses the minimum requirement for AES is a N is a value of 128 so that the key has a length of 128 bits and blocks about 128 blocks (1.1 Background).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a key with a bit size of 128 and 128 block size. One of ordinary skill in the art would have been motivated to do this because the minimum requirements for AES are a key size of 128 and the processor used to test AES candidates is a 32 bit processor. AES is a system that will be used to secure sensitive government information (Nechvatal 1. Overview of the Development Process for the Advanced Encryption Standard and Summary of Round 2 Evaluations) and as a result will greatly influence other systems for securing information.

In reference to claim 15 wherein the encryption module is a ROM-based encryption module comprising a plurality of ROMs for storing algorithms corresponding to the plurality of encryption operations and related application programs.

Garcken does not teach a system wherein the encryption module is a ROM-based encryption module comprising a plurality of ROMs for storing algorithms corresponding to the plurality of encryption operations and related application programs.

Nechvatal discloses the Rijndael (Section 3.4.1.1 Notes on the Finalists) algorithm as being the most efficient algorithm and yet uses twice as much ROM for the algorithm.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to a plurality of ROMs for storing algorithms corresponding to the plurality of encryption operations and related application programs as in Nechvatal in the system of Garcken. One of ordinary skill in the art would have been motivated to do this because the most efficient algorithm uses mostly ROM and therefore it is more efficient to utilize ROM (Section 3.4.1.1 Notes on the Finalists).

Claims 3 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Garcken et al in view of Oomori et al (6,891,950 B1).

In reference to claims 3 and 11 wherein the digital data processing module in the inverse key evaluation module is electrically connected to the m XOR logic gates, the digital data processing module comprising : a byte rotator for inverting the order of a plurality of bytes in the N-bit key; a byte substituter electrically connected to the byte rotator for substituting a plurality of predetermined byte for the bytes in the N-bit key; and a byte disturber for generating a disturbing value according to a predetermined disturbing table and utilizing the disturbing value to perform an XOR operation with the N-bit key.

Although Garcken discloses a key stored in a key register and the formation of n-bit S Tables for use in encryption, Garcken does not discloses a byte rotator for inverting the order of a plurality of bytes in the N-bit key; a byte substituter electrically connected to the byte rotator for substituting a plurality of predetermined byte for the bytes in the N-bit key; and a byte disturber for generating a disturbing value according to a predetermined disturbing table and utilizing the disturbing value to perform an XOR operation with the N-bit key.

Oomori discloses a byte rotator for inverting the order of a plurality of bytes in the N-bit key (column 7 lines 5-24); a byte substituter, s-box, (column 5 lines 60-67) electrically connected to the byte rotator for substituting a plurality of predetermined byte for the bytes in the N-bit key (column 5 lines 30-35), the s-box stands for substitution box and performs the substitution function; and a byte disturber for generating a disturbing value according to a predetermined disturbing table and utilizing the disturbing value to perform an XOR operation with the N-bit key (parts 15 and 16 Fig. 3). The key expander performs the task of the byte distributer by performing a shift and then addition step wherein the disturbing value is the rotated key. The value is then used for the XOR in the next stage (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a rotator, substituter, and distributer of the key generation of Oomori in the block cipher of Garcken. One of ordinary skill in the art would have been motivated to do this because the extended key generation method can improve randomness of extended keys while suppressing an increase in apparatus price and circuit scale and preventing generation of week keys, and can improve cryptological robustness (column 3 lines 44-51).

Claims 6, 13, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gracken in view of Nechvatal as applied to claim 5 above, and further in view of the article by Do ("WAP Security: WTLS").

In reference of claims 6, 13, and 19 wherein the crypto-system is applied to a wireless LAN.

Garcken does not expressly disclose the crypto-system is applied to a wireless LAN.

Do discloses a system that supports block cipher algorithms (Comparison between WTLS and SSL).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use block ciphers in a wireless network as in Do in the system of Garcken. One of ordinary skill in the art would have been motivated to do this because wireless systems allow users to access many transaction-based activities (Introduction Do).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PWK
Tuesday, November 14, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100